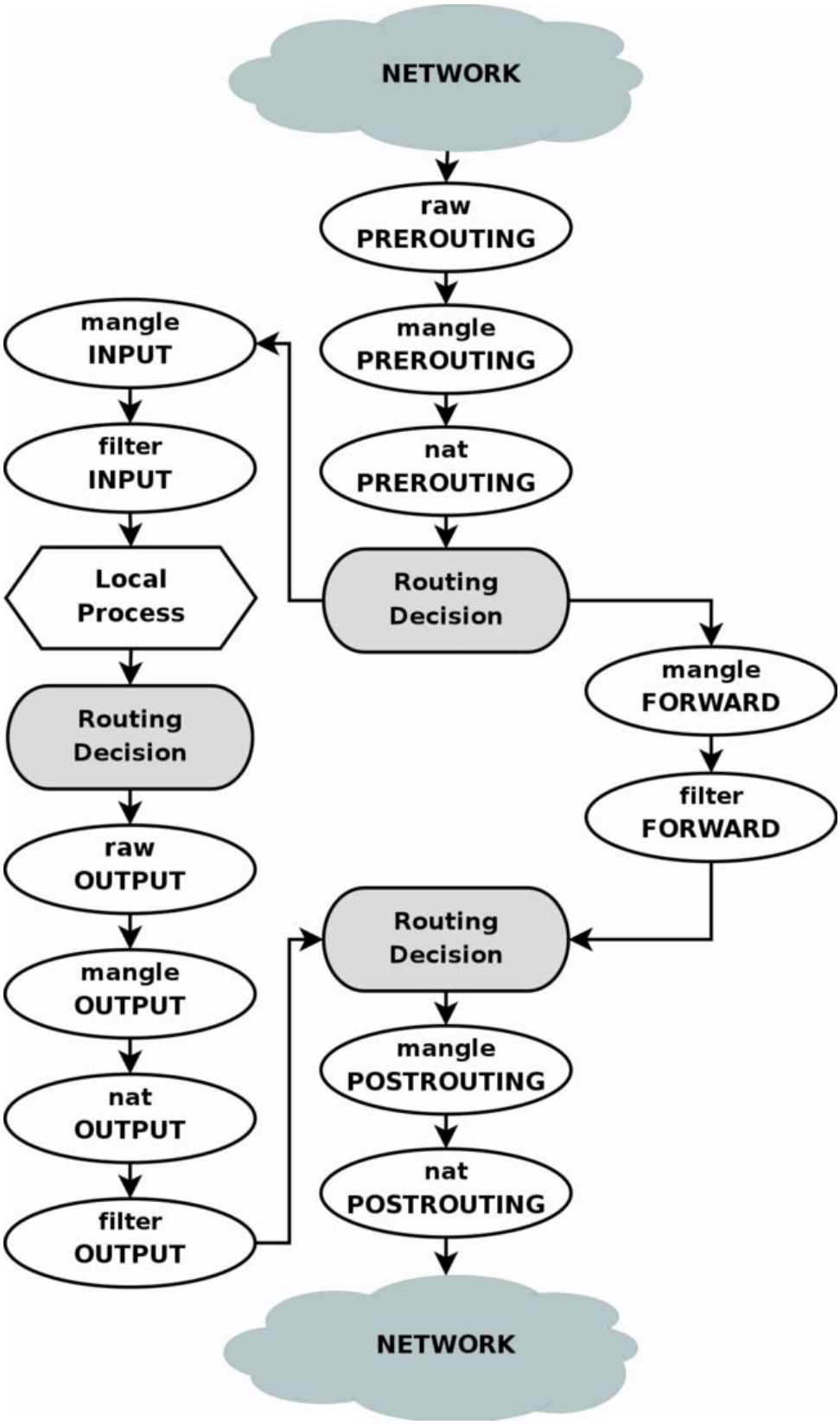

Schema gestione pacchetti di un host all'interno del kernel Linux da parte del sistema Netfilter.

Notare la presenza della rete da cui possono essere ricevuti pacchetti diretti a processi del nostro stesso host oppure diretti ad altri hosts.

Notare la presenza dei processi locali che possono ricevere e generare pacchetti.

Notare le **Table**:
filter, nat,
mangle, raw.
che rappresentano le classi di operazioni a cui può essere sottoposto un pacchetto.

Notare le **Chain**:
PREROUTING,
FORWARD,
POSTROUTING,
INPUT,
OUTPUT,
che rappresentano le fasi di vita del pacchetto durante le quali il pacchetto può essere intercettato.

---

esempio di intercettazione di pacchetti contenenti TCP
che escono dall'interfaccia eth0
a cui vengono modificati l'indirizzo IP e la porta mittenti
mettendo quelli indicati nell'intervalo --to-source.
Analogamente, anche i pacchetti della stesse connessioni TCP
che seguono il percorso al contrario (cioe' entrano da eth0)
vengono nattate al contrario, cioe' vengono messi come
nuovo indirizzo IP e porta destinatari
quelli che erano l'indirizzo IP e porta del mittente
prima del cambiamento.

iptables -t nat -A POSTROUTING -p tcp -o eth0 -j SNAT --to-source 194.236.50.155-194.236.50.160:1024-32000

---

visualizzazione delle regole presenti nella tabella mangle

```
iptables -t mangle --list -n
```

---

script per eliminazione di tutte le regole presenti nelle tabelle nat, filter e mangle

```
#!/bin/sh

echo elimino tutte le precedenti regole di iptables
iptables -t nat -F
iptables -t mangle -F
iptables -t filter -F
```

---

script per passare ad una applicazione locale tutti i datagram UDP
generati da una altra applicazione locale

```
#!/bin/sh

echo redireziono i pkt UDP generati localmente verso la mia applicazione
addspaceudp

iptables -t mangle -A OUTPUT -p udp -j QUEUE
```
